(19) BUNDESREPUBLIK DEUTSCHLAND

DEUTSCHES PATENT- UND MARKENAMT

(12) **Offenlegungsschrift**

(10) **DE 101 04 409 A 1**

(51) Int. Cl.[7]:
H 04 L 12/28
H 04 L 29/12
H 04 M 1/737
H 04 Q 7/32

(21) Aktenzeichen: 101 04 409.7
(22) Anmeldetag: 1. 2. 2001
(43) Offenlegungstag: 29. 8. 2002

(71) Anmelder:
Wincor Nixdorf GmbH & Co. KG, 33106 Paderborn, DE

(72) Erfinder:
Kremer, Holger, 33175 Bad Lippspringe, DE

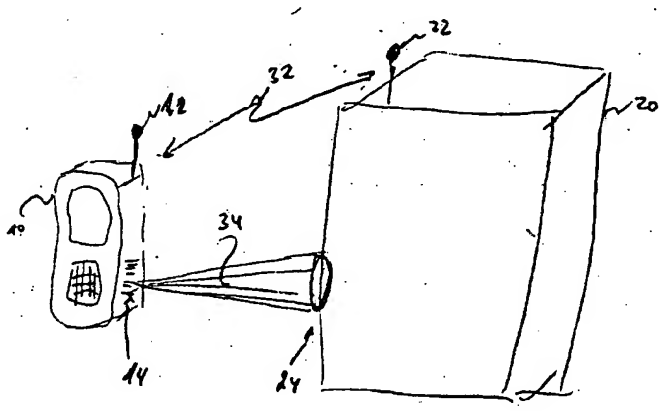
(56) Entgegenhaltungen:
DE 100 25 017 A1
DE 6 92 22 911 T2

Die folgenden Angaben sind den vom Anmelder eingereichten Unterlagen entnommen

Prüfungsantrag gem. § 44 PatG ist gestellt

(54) Verbindungsauswahl über einen optischen Code

(57) Methode und Geräte zum Aufbauen einer drahtlosen Verbindung zwischen einem ersten und einem zweiten Gerät, wobei daß das erste Gerät mittels einer Leseeinrichtung ein außen an dem zweiten Gerät sichtbaren optischen Code liest, welcher zudem in dem zweiten Gerät elektronisch gespeichert ist, und beim Aufbau der Verbindung mittels dieses Codes sicherstellt, daß die Identität der beiden Geräte gesichert wird.



DE 101 04 409 A 1

DE 101 04 409 A 1

Beschreibung

Technisches Gebiet

[0001] Die Erfindung betrifft eine Einrichtung, mit der beim Aufbau einer drahtlosen Verbindung die Identität der Teilnehmer gesichert wird.

[0002] Es wurde vorgeschlagen, bei Kassen und Selbstbedienungsgeräten zumindest einen Teil der Interaktion mit dem Benutzer über ein mobiles Gerät abzuwickeln. Hierzu gehört sowohl die eigentliche Bedienung, z. B. eines Geldausgabeautomaten, als auch beispielsweise die Bezahlfunktion an einer Kasse. Die Datenverbindung zu dem mobilen Gerät erfolgt bevorzugt über eine unter der Bezeichnung 'Bluetooth' bekannten Schnittstelle für drahtlose Funkübertragung. Im folgenden wird stellvertretend für ein mobiles Gerät mit Verarbeitungsfähigkeiten und einer Schnittstelle für drahtlose Datenübertragung ein Mobiltelefon mit Bluetooth-Transceiver angenommen.

[0003] Im Gegensatz zu der drahtlosen Verbindung nach dem IrDA-Standard, die mit Infrarotlicht arbeitet, ist eine Funkübertragung praktisch ungerichtet. Daher sieht die Bluetooth-Schnittstelle eine Geräte-Identifikation vor, so daß gezielt eine Verbindung zu einem Gerät der gewünschten Klasse erfolgen kann. Durch diese Methode ist an einem Arbeitsplatz oder im häuslichen Bereich das Problem der Geräte-Identifikation als gelöst anzusehen.

[0004] Bei mehreren gleichartigen Geräten jedoch sind weitere Maßnahmen notwendig. Beispielsweise ist eine Bezahlfunktion durch ein Mobiltelefon mit Bluetooth-Schnittstelle vor einer Kasse in einem Supermarkt auszulösen. Zum einen ist sicherzustellen, daß kein Mobiltelefon eines noch wartenden Kunden zu der Bezahlung verbunden wird. Dies kann einfach dadurch erreicht werden, daß der Kunde an seinem Mobiltelefon die Zahlungsfunktion einleitet. Da aber weitere Kassen in Funkreichweite sein können, ist immer noch unklar, mit welcher der Kassen das Bezahlprotokoll abgewickelt werden soll. Die naheliegende Lösung ist es, auf dem Mobiltelefon ein Auswahlmenü mit den Nummern der Kassen anzuzeigen, die zur Bezahlung anstehen. Diese Lösung ist nicht nur umständlich und zeitaufwendig. Da Kollisionen relativ selten sind, wird der Benutzer häufig irrtümlich die erste Kasse der Liste bestätigen, was langfristig zu Akzeptanzproblemen führen kann. Es ist ferner zu berücksichtigen, daß bei allen Lösungen insbesondere im Kassenbereich wenig Zeit zur Verfügung steht.

[0005] Gesucht ist daher ein Weg, schnell und eindeutig eine Zuordnung zwischen mobilem und stationärem Gerät zu bewirken.

[0006] Die Erfindung verwendet hierzu eine außen auf dem mobilen Gerät sichtbare oder angezeigte optische Markierung, bevorzugt einen Strichcode. Bei Kassen ist meist ohnehin ein Strichcode-Leser vorhanden, der dann zum Lesen dieser Markierung mit verwendet werden kann.

[0007] Alternativ kann auch an der Kasse ein Code aufgebracht sein und das mobile Gerät mit einem Strichcode-Leser versehen werden, wie er aus Fernbedienungen von Videorecordern bekannt ist.

[0008] Weitere Merkmale und Vorteile der Erfindung ergeben sich aus der folgenden Beschreibung, welche in Verbindung mit den beigefügten Zeichnungen die Erfindung an Hand eines Ausführungsbeispiels erläutert.

Kurzbeschreibung der Zeichnungen

[0009] Es zeigt

[0010] Fig. 1 symbolisch eine Anordnung, in der die Erfindung benutzt wird.

Beschreibung einer Ausführungsform der Erfindung

[0011] In Fig. 1 ist eine Anordnung symbolisiert, in der die Erfindung benutzt wird.

[0012] Ein mobiles Gerät, hier als Mobiltelefon **10** dargestellt, verfügt über eine Schnittstelle für eine drahtlose Verbindung, insbesondere ein Nahfeld-Funknetzwerk wie Bluetooth. Diese Einrichtung ist durch eine Antenne **12** symbolisiert. Bei einem Mobiltelefon sind demnach zwei drahtlose Verbindungen und zwei Antennen vorhanden; eine nicht gezeigte für die Verbindung für mobile Telefonie und die gezeigte für das Funknetzwerk. Im übrigen ist bei modernen Funktelefonen keine der beiden Antennen als Stabantenne ausgeführt, so daß diese Symbolisierung angemessen erscheint.

[0013] Ferner ist an dem mobilen Gerät ein optischer Code angebracht, hier als Strichcode **14** an der Seite dargestellt.

[0014] Weiterhin ist ein stationäres Gerät **20** gezeigt, das gleichfalls über eine Schnittstelle für eine drahtlose Verbindung verfügt, die der von dem mobilen Gerät verwendeten entspricht und gleichfalls durch eine Antenne **22** symbolisiert ist.

[0015] Ferner verfügt das stationäre Gerät **20** über eine Abtasteinrichtung **24**, mit der, hier durch ein Strahlenbündel **34** symbolisiert, der Barcode **14** an dem mobilen Gerät **10** abgetastet wird.

[0016] Bei einer Ausführungsform der Erfindung stellt der Code auf dem mobilen Gerät die Netzwerkadresse des mobilen Geräts dar. In Netzwerksystemen ist es verbreitet, daß jeder Sende-Empfänger ('transceiver') eine eindeutige Adresse auf der untersten Ebene der Kommunikationsprotokolle, dem 'media access'-Layer, besitzt, die daher auch als MAC-Adresse bezeichnet wird. Ein geeignete Software im stationären Gerät wird daher nach dem Lesen des optischen Codes eine Verbindung zu genau dieser Adresse aufbauen und damit die Identität des mobilen Geräts sicherstellen. Um die Identität des stationären Geräts zu sichern, kann das mobile Gerät einen Verbindungaufbau darauf beschränken, daß dieser ohne vorherige Adressermittlung direkt mit der MAC-Adresse erfolgt.

[0017] Die Verwendung der MAC-Adresse hat insbesondere den Vorteil, daß dieser weltweit eindeutig ist und daher Kollisionen praktisch vollständig ausgeschlossen sind. Alternativ kann auch eine Netzwerkadresse aus anderen Schichten verwendet werden, insbesondere eine IP-Adresse, was mit Einführung von der Version 6 der Internetprotokolle wieder praktikabel wird.

[0018] Falls jedoch die Codierung der Netzwerkadresse nicht zweckmäßig ist, kann auch ein beliebiger anderer Code verwendet werden. Die Codierung der Netzwerkadresse kann insbesondere dann unzweckmäßig sein, wenn entweder die Netzwerksoftware deren Verwendung nicht oder schlecht unterstützt oder der Strichcode der Netzwerkadresse zu viel Platz auf einem kleinen Mobiltelefon beanspruchen würde oder eine Weitergabe dieses Codes aus anderen Gründen nicht erwünscht ist. Hierzu kann auch ein Code verwendet werden, der mittels einer Datenbank in die Netzwerkadresse umgewandelt wird.

[0019] Eine andere Alternative besteht darin, die Telefonnummer des Besitzers zu codieren. Auch dieser Code ist hinreichend eindeutig und weniger lang. Bei einem Mobiltelefon kann es ohnehin zweckmäßig sein, die relativ langen Nummern per Aufkleber maschinenlesbar zu machen.

[0020] In diesen Fällen, in denen der Code nicht eine Netzwerkadresse direkt darstellt, wird im Rahmen des Verbindungsaufbaus dieser Code übermittelt und überprüft. Dabei ist es unerheblich, welches Gerät den Code sendet und

welches ihn vergleicht. Dies kann sowohl das die Verbindung initiierende Gerät als auch das gerufene Gerät, die Gegenstelle, sein. Der Code kann bereit mit dem Ruf übertragen oder in der Antwort des gerufenen Geräts enthalten sein.

[0021] Im Bluetooth-Netzwerk sind kryptographische Maßnahmen für die Sicherung des Datenverkehrs enthalten; das Schlüsselmanagement jedoch ist den Anwendungsschichten überlassen. Hier kann der Code in das Schlüsselmanagement integriert werden. Wird ein zufälliger Code verwendet, so kann dieser einfach zur Verschlüsslung der Kommunikation verwendet werden und so ohne weitere Maßnahmen bereits ein hohes Maß an Sicherheit gegen Abhören, Verfälschen und Vorspiegelung falscher Identität gewonnen werden. Obwohl dieser Sitzungsschlüssel nicht als sonderlich geheim anzusehen ist, erfordert ein gezielter Mißbrauch einen erheblichen Aufwand, der meist als prohibitiv hoch anzusehen ist. Selbstverständlich sollte ein solcher Code nicht zur Authentisierung einer Zahlung dienen.

[0022] Anstelle von einem zufälligen Code kann auch der öffentliche Schlüssel eines Schlüsselpaares bei asymmetrischer Verschlüsslung codiert sein, auch wenn dieser mit z. B. 1024 Bit oder 128 Byte länger als eine V6-Internet-Adresse ist. Dessen Verwendung rechtfertigt sich gegebenenfalls aus dem Zusatznutzen, daß einem Gesprächspartner auf einfach Art so der öffentliche Schlüssel für vertrauliche elektronische Kommunikation übergeben werden kann. Eine Variante benutzt eine Prüfsumme, üblicherweise als 'fingerprint' bezeichnet, eines öffentlichen Schlüssels, bzw. einen Teil davon und ermöglicht so die Verifizierung eines öffentlichen Schlüssels als Zusatznutzen.

[0023] Wird auf den Zusatznutzen verzichtet, so kann wegen der geringen Exposition und des relativ geringen Risikos auch ein speziell für diesen Fall gewähltes Schlüsselpaar mit geringer Bitlänge von z. B. 64 Bit entsprechend 22 Dezimalziffern gewählt werden, dessen privater Teil in dem mobilen Gerät gespeichert ist. Das stationäre Gerät verschüsselt einen neuen Sitzungsschlüssel mit dem gelesenen Code als öffentlichem Schlüssel und schickt das Ergebnis an das mobile Gerät, welches damit den Sitzungsschlüssel decodiert. Diese Hinweise sollen hier nur als Beispiel für die Integration des gelesenen Codes in das Schlüsselmanagement dienen.

[0024] Die Länge des Codes und der Grad seiner Zufälligkeit wird nach pragmatischen Gesichtspunkten oder normativen Vorgaben zu wählen sein. Lediglich vier Ziffern, insbesondere das Geburtsdatum ohne Jahr, dürfte wegen der Wahrscheinlichkeit einer Kollision, die beim Geburtsdatum ca. 1 : 30 beträgt, nicht ausreichend sein. Bevorzugt wird daher eine ohnehin eindeutige oder quasi-eindeutige Bezeichnung wie die Telefonnummer oder die Passnummer verwendet werden.

[0025] Die Erfindung wurde am einem Beispiel dargestellt, bei dem ein mobiles Gerät die optische Markierung trägt und ein stationäres Gerät den Leser für die Markierung umfaßt. Dies ist meistens dann sinnvoll, wenn die Anzahl der mobilen Geräte wesentlich größer als die der stationären Geräte ist. Zudem ist die Energieversorgung bei einem stationären Gerät einfacher. Die Erfindung umfaßt jedoch auch den umgekehrten Fall, bei dem die Markierung auf dem stationären Gerät angebracht und der optische Leser in dem mobilen Gerät vorgesehen ist. Da beispielsweise Selbstbedienungsgeräte, z. B. Geldautomaten, normalerweise nicht über einen Barcode-Scanner verfügen, wird hier das mobile Gerät den Leser umfassen. Ein Barcode kann an einem Automaten dieser Art problemlos angebracht und ggf. erneuert werden.

[0026] Auch kann es für die Akzeptanz sinnvoll sein, daß das mobile Gerät die Adresse liest und von sich aus die Verbindung aufbaut. Im Falle der Bezahlung an einer Kasse ist es damit dem Ladeninhaber überlassen, daß die durch diesen Code veranlaßten Zahlung den richtigen Empfänger erreicht. Hier kann der Code auch besonders kurz sein, da nur eine kleine Zahl von stationären Geräten unterschieden werden muß.

[0027] Bei dem oben beschriebenen Fall eines speziell für diesen Fall bereitgestellten Schlüssels für asymmetrische Verschüsslung, dessen öffentlicher Teil auf dem mobilen Gerät codiert ist, liegt die Sicherung der Identität darin, daß das stationäre Gerät sicher sein kann, daß das mobile Gerät dasjenige ist, dessen Code gelesen wurde. Im Falle eines Geldautomaten und aus Sicht seiner Betreiber ist diese Variante vorzuziehen. In dem zuletzt dargestellten Fall, in dem die Leseeinrichtung an dem mobilen Gerät vorgesehen ist, ist daher umgekehrt die Identität des stationären Geräts gesichert. Dies könnte bei Kassen die bevorzugte Ausprägung sein.

[0028] Passende Strichcode-Leser geringer Leistungsaufnahme sind allgemein bekannt, insbesondere von Fernbedienungen für Videorecorder.

[0029] Der Anschaulichkeit halber wurde die Erfindung an Hand von Strichcodes als bevorzugter optischer Codierung beschrieben. Selbstverständlich sind andere Codes, z. B. OCR-Zeichen, gleichfalls verwendbar.

Patentansprüche

1. Methode zum Aufbauen einer drahtlosen Verbindung zwischen einem erstem und einem zweiten Gerät, **dadurch gekennzeichnet**, daß das erste Gerät mittels einer Leseeinrichtung einen außen an dem zweiten Gerät sichtbaren optischen Code liest, daß der Code oder ein dem Code eindeutig zugeordneter Wert in dem zweiten Gerät elektronisch gespeichert ist, und beim Aufbau der Verbindung mittels dieses Codes die Identität der Teilnehmer der Verbindung gesichert wird.
2. Methode nach Anspruch 1, wobei für die drahtlose Verbindung ein Nahfeld-Funknetzwerk, insbesondere nach dem Bluetooth-Standard, verwendet wird.
3. Methode nach Anspruch 2, wobei der gelesene Code die Netzwerkadresse des zweiten Geräts ist oder letztere über eine Datenbank aus dem gelesenen Code bestimmt wird.
4. Methode nach Anspruch 1, wobei das erste Gerät von dem zweiten Gerät den Code empfängt und mit dem gelesenen vergleicht.
5. Methode nach Anspruch 1, wobei das zweite Gerät den gelesenen Code von dem ersten Gerät empfängt und mit dem gespeicherten vergleicht.
6. Methode nach einem der Ansprüche 4 oder 5, wobei als Code eine einer Person zugeordnete Nummer, z. B. Telefonnummer, Passnummer oder Geburtsdatum, oder ein Teil davon, ist.
7. Methode nach einem der vorhergehenden Anspüche, wobei der Code für das Schlüsselmanagement einer verschlüsselten Verbindung verwendet wird.
8. Methode nach Anspruch 7, wobei der an dem zweiten Gerät sichtbaren Code den öffentlichen Teil eines Schlüsselpaares für asymmetrische Verschlüsslung bereitstellt und dessen geheimer Teil in dem zweiten Gerät gespeichert ist.
9. Methode nach Anspruch 8, wobei das erste Gerät einen zufälligen Sitzungsschlüssel mit dem gelesenen Code verschlüsselt, an das zweite Gerät sendet und dieses den Sitzungsschlüssel mittels des gespeicherten geheimen Teils rekonstruiert.
10. Methode nach einem der vorhergehenden Ansprü-

che, wobei der Code als Strichcode dargestellt ist.

11. Gerät mit einer Schnittstelle für eine drahtlose Verbindung, dadurch gekennzeichnet, das das Gerät eine optische Leseeinrichtung umfaßt und Mittel enthält, um mit der optischen Leseeinrichtung einen Code zu lesen und mittels dieses Codes die Identität einer Gegenstelle der Verbindung zu sichern.

12. Gerät nach Anspruch 11, wobei für die drahtlose Verbindung ein Nahfeld-Funknetzwerk, insbesondere nach dem Bluetooth-Standard, verwendet wird.

13. Gerät nach Anspruch 12, wobei der gelesene Code die Netzwerkadresse der Gegenstelle ist oder letztere über eine Datenbank aus dem gelesenen Code bestimmt wird.

14. Gerät nach Anspruch 11, wobei das Gerät von der Gegenstelle den Code empfängt und mit dem gelesenen vergleicht.

15. Gerät nach Anspruch 11, wobei das Gerät den gelesenen Code an die Gegenstelle sendet.

16. Gerät nach einem der Ansprüche 14 oder 15, wobei als Code eine einer Person zugeordnete Nummer, z. B. Telefonnummer, Passnummer oder Geburtsdatum, oder ein Teil davon, ist.

17. Gerät nach Anspruch 11, wobei der Code für das Schlüsselmanagement einer verschlüsselten Verbindung verwendet wird.

18. Gerät nach Anspruch 17, wobei der gelesene Code als öffentlicher Teil eines Schlüsselpaars für asymmetrischer Verschlüsslung benutzt wird.

19. Gerät nach Anspruch 18, wobei das Gerät einen zufälligen Sitzungsschlüssel mit dem gelesenen Code verschlüsselt und an die Gegenstelle sendet.

20. Gerät nach einem der Ansprüche 11 bis 19, wobei der Code als Strichcode dargestellt ist.

21. Gerät mit einer Schnittstelle für eine drahtlose Verbindung, dadurch gekennzeichnet, daß außen an dem Gerät ein optischer Code sichtbar ist, der Code oder ein dem Code eindeutig zugeordneter Wert in dem Gerät elektronisch gespeichert ist und das Gerät Mittel umfaßt, mit denen an Hand des Codes die Identität der Gegenstelle der Verbindung gesichert wird.

22. Gerät nach Anspruch 21, wobei für die drahtlose Verbindung ein Nahfeld-Funknetzwerk, insbesondere nach dem Bluetooth-Standard, verwendet wird.

23. Gerät nach Anspruch 22, wobei der gelesene Code die Netzwerkadresse der Gegenstelle ist oder über eine Datenbank aus dem gelesene Code wird.

24. Gerät nach Anspruch 21, wobei das Gerät von der Gegenstelle den Code empfängt und mit dem gespeicherten vergleicht.

25. Gerät nach Anspruch 21, wobei das Gerät den gespeicherten Code an die Gegenstelle sendet.

26. Gerät nach einem der Ansprüche 24 oder 25, wobei als Code eine einer Person zugeordnete Nummer, z. B. Telefonnummer, Passnummer oder Geburtsdatum, oder ein Teil davon, ist.

27. Gerät nach einem der Anspüche 21 bis 26, wobei der Code für das Schlüsselmanagement einer verschlüsselten Verbindung verwendet wird.

28. Gerät nach Anspruch 27, wobei der sichtbare Code den öffentlichen Teil eines Schlüsselpaares für asymmetrische Verschlüsslung darstellt, dessen geheimer Teil in dem Gerät gespeichert ist.

29. Gerät nach Anspruch 28, wobei das Gerät von der Gegenstelle Daten empfängt, die als mit dem öffentlichen Teil verschlüsselten zufälligen Sitzungsschlüssel behandelt werden, welcher mittels des gespeicherten geheimen Teils rekonstruiert wird.

30. Gerät nach einem der Ansprüche 21 bis 29, wobei der Code als Strichcode dargestellt ist.

31. Software für ein Gerät oder eine Methode nach einem der vorhergehenden Ansprüche als Teil der Mittel, mit denen die Identität der Teilnehmer der Verbindung gesichert wird.

Hierzu 1 Seite(n) Zeichnungen

- Leerseite -

Nummer: DE 101 04 409 A1
Int. Cl.[7]: H 04 L 12/28
Offenlegungstag: 29. August 2002

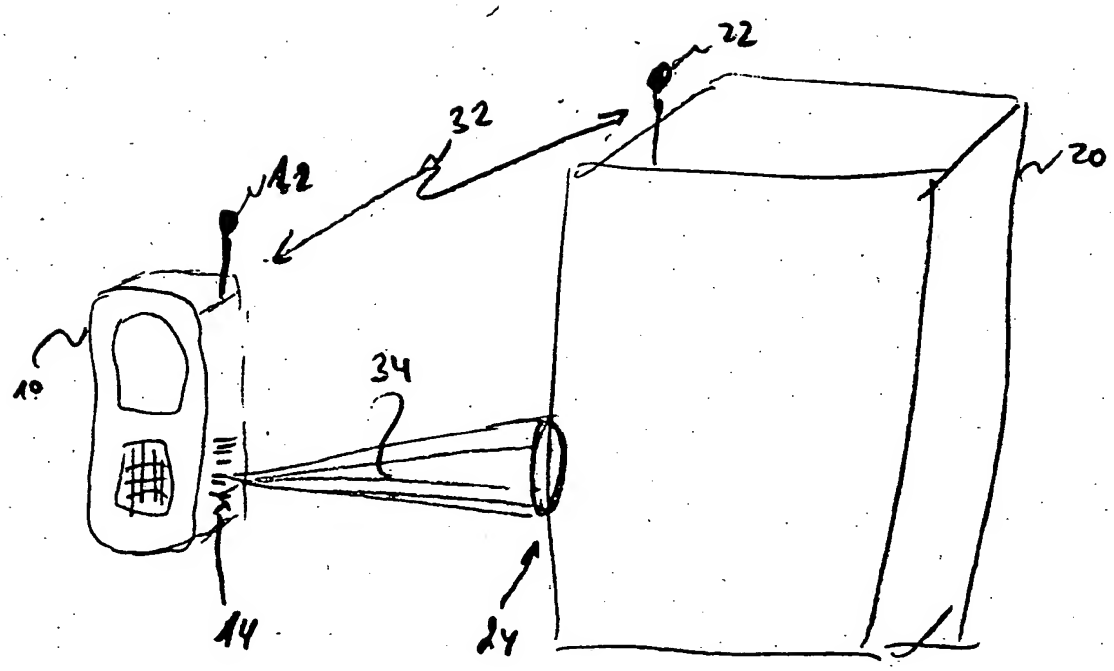


Fig. 1

DOCKET NO: DSC-AP-204
SERIAL NO: _____
APPLICANT: Churt et al.

LERNER AND GREENBERG P.A.
P.O. BOX 2480
HOLLYWOOD, FLORIDA 33022
TEL. (954) 925-1100